УДК 004.7:37

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ В НАУКОВИХ УСТАНОВАХ НАПН УКРАЇНИ

Іван Голуб,
науковий співробітник
відділу цифрових освітніх ресурсів
Інститут професійної освіти НАПН України,
https://orcid.org/0000-0001-9008-6255
e-mail: golub.ivan@gmail.com

Анотація. У статті здійснено огляд і узагальнення основних складових інформаційної інфраструктури та інформаційних ресурсів у типових наукових установах Національної академії педагогічних наук України (НАПН України). Аналізуються сучасний стан, структура та напрямки розвитку інформаційних систем, наявна електронна база й особливості організації доступу до наукових даних і ресурсів у вітчизняних установах. Окрему увагу приділено адаптації інформаційної інфраструктури до умов воєнного часу в Україні, що є надзвичайно важливим для забезпечення безперервності наукової діяльності, збереження та захисту інтелектуального потенціалу держави.

Ключові слова: інформаційна інфраструктура, інформаційні ресурси, наукові установи НАПН України, електронні бази даних, наукова діяльність під час війни.

GENERAL CHARACTERISTICS OF THE INFORMATION INFRASTRUCTURE IN SCIENTIFIC INSTITUTIONS OF THE NATIONAL ACADEMY OF EDUCATIONAL SCIENCES OF UKRAINE

Ivan Golub,
Researcher of Department of Digital Educational Resources of the Institute of Vocational Education of the NAES of Ukraine

Abstract. The article reviews and summarizes the main components of the information infrastructure and information resources in typical scientific institutions of the National Academy of Educational Sciences of Ukraine (NAES of Ukraine). The current state, structure, and development trends of informational systems, the available electronic database, and peculiarities of organizing access to scientific data and resources in Ukrainian institutions are analyzed. Special attention is paid to the adaptation of information infrastructure during wartime in Ukraine, highlighting its critical importance for ensuring the continuity of scientific work and protecting the nation's intellectual potential.

Keywords: information infrastructure, information resources, NAES scientific institutions, electronic databases, scientific activity during war.

Наукові установи Національної академії педагогічних наук України (НАПН України) є одними з ключових осередків формування, опрацювання, збереження та поширення інформаційних педагогічних, психологічних, інформаційно-аналітичних ресурсів, що забезпечують підтримку наукових досліджень і освітнього процесу. Інформаційна інфраструктура таких установ охоплює різноманітні цифрові системи, електронні бази даних наукових публікацій, навчальні платформи та сервіси доступу, створюючи сприятливі умови для ефективної наукової взаємодії. В умовах військового стану в Україні, захист та безперервна підтримка інформаційних ресурсів набувають особливого значення, потребуючи врахування специфіки академічного середовища, відкритості наукового доступу та інтеграції з зовнішніми платформами.

НАПН України є провідною науковою організацією, що займається дослідженнями в галузі освіти, педагогіки та психології (Міністерство освіти і науки України, 2023). Станом на 2019 р. в її наукових установах працювало 1060 науковців, серед яких 190 докторів наук і 484 кандидатів наук (Національна академія педагогічних наук України, n.d.). Офіційний сайт НАПН України https://naps.gov.ua.

Інформація про кількість працівників на посаді інженера комп'ютерних мереж, ІТ-фахівців, системних адміністраторів в офіційних джерелах НАПН України наразі не зазначається. З огляду на те, що основна діяльність академії пов'язана з гуманітарними науками, кількість таких спеціалістів, ймовірно, є незначною. Якщо в штаті й присутні інженери комп'ютерних систем, то питаннями кіберзахисту вони не займаються. ІТ-підрозділ в академії також відсутній.

Застосування в наукових установах рекомендацій з кібербезпеки наразі обмежене через відсутність внутрішніх актів, кадрового ресурсу та достатнього фінансування. Проблема не зникає і залишається актуальною. Так, після 2022 р. з'явилися специфічні дослідження, зокрема:

Kovalenko & Lysenko (2023) – аналіз атак на науку в Україні;

Shevchenk et al. (2024) – про кіберстійкість освітніх установ;

Datsyuk & Vrnva (2025) – про післявоєнні моделі захисту науки;

Shkuropadska D. et al. (2025) – дані про кібербезпеку, цифрову інфраструктуру та соціально-економічний вплив;

Shtantsel S. et al. (2025) – стратегії інформаційної безпеки в державному секторі, їх ефективнвсть та ризики кібербезпеки.

Наведені праці досліджують цифрову стійкість та кібербезпеку, зокрема в контексті України та Східної Європи. В них обговорюються виклики швидкої цифровізації, включаючи кіберзагрози та цифровий розрив. У текстах підкреслюється зростаюча залежність від технологій і необхідність зміцнення цифрової інфраструктури. Їх автори також аналізують роль державних органів, приватного сектору та громадянського суспільства у забезпеченні кібербезпеки, зокрема в Україні під час російської агресії, де активно залучаються кіберволонтери та досліджуються правові аспекти використання кіберзброї. Здійснюється порівняльний аналіз ефективності кіберзахисту різних країн та вивчається, як великі мовні моделі можуть посилювати загрози, такі як фішинг.

Установи НАПН України виконують важливу роль у розвитку освітніх технологій, психолого-педагогічних досліджень та цифровізації освіти. Водночас із зростанням цифрової активності та накопиченням критично важливої інформації підвищуються й ризики кіберзагроз. Проведений аналіз дає змогу виявити ключові особливості й проблеми сучасного стану кіберзахисту в наукових установах, що мають власну інформаційну інфраструктуру, яка забезпечує проведення досліджень, управління науковою діяльністю, облік ресурсів та взаємодію з освітньою спільнотою. Така інфраструктура включає технічні, програмні та інформаційні компоненти, що забезпечують безперервність функціонування установ і реалізацію їхнього науково-освітнього потенціалу.

Установи НАПН України (Інститут психології, Інститут педагогіки, Інститут професійної освіти, Інститут педагогічної освіти і освіти дорослих та ін.) мають у своєму розпорядженні: офіційні сайти

з публікацією результатів досліджень; наукові електронні бібліотеки та архіви; вебплатформи для дистанційного навчання; внутрішні файлові сховища; email-сервери на власних доменах; хмарні акаунти в Google Workspace, Microsoft 365.

Ці ресурси є критично важливими активами, і мають значні ризики втрати інформації, отримання репутаційних збитків та зупинки освітніх процесів.

З метою збору емпіричних даних було проведено опитування 30 наукових співробітників установ НАПН України щодо визначення їхньої обізнаності стосовно наявних політик безпеки в установі, розуміння наявності загроз, а також заохотити їх до покращення своїх знань з кібербезпеки, кіберзахисту та кібергігієни. Анкета включала 4 питання з варіантами відповіді:

1. Наукова установа в якій ви працюєте має внутрішню політику кібербезпеки? (варіанти відповіді: так, ні, не знаю)?

2. Ви часто робите резервні копії своїх робочих документів в установі? (варіанти відповіді: часто, інколи, ніколи) ?

3. Ви проходили навчання з кібербезпеки, кіберзахисту або кібергігієни і чиїм коштом воно було сплачено? (варіанти відповіді: наукова установа сплатила моє навчання; проходив власним коштом; не проходив).

4. Вам відомо про кіберінциденти у вашій науковій установі (варіанти відповіді: так; ні)?

5. Як часто кіберінциденти мали місце у вашій науковій установі за останні 12 місяців (варіанти відповіді: часто, не часто, ніколи)?

Отримано наступний розподіл відповідей респондентів (табл. 1).

Таблиця 1

Результати опитування респондентів

Варіант відповіді	***Кількість***	***Відсоток***
1. Наявність внутрішньої політики кібербезпеки		
Так	0	0%
Ні	13	43,3%
Не знаю	17	56,7%
2. Резервне копіювання документів		
Часто	1	3,3%
Іноді	23	76,7%
Ніколи	6	20%

Продовження табл. 1

Варіант відповіді	***Кількість***	***Відсоток***
3. Проходження навчання з кібербезпеки		
За кошт установи	0	0%
Проходив власним коштом	9	30%
Не проходив	21	70%
4. Обізнаність про кіберінциденти		
Так	13	43,3%
Ні	17	56,7%
5. Частота кіберінцидентів за останні 12 місяців		
Часто	3	10%
Не часто	17	56,7%
Ніколи	10	33,3%

Результати дослідження свідчать про наступне: жоден з опитаних не підтвердив наявність політики кібербезпеки, понад половини – взагалі не знає про її існування. Лише 1 особа регулярно виконує резервне копіювання, що свідчить про низький рівень захисту робочої інформації. 30% учасників мають базову підготовку, яку здобуто за власний кошт. Жодного випадку підтримки з боку установи. Більшість працівників не знають про кіберінциденти в установі, що може свідчити про відсутність комунікації чи моніторингу.

Висновок. Наукові установи НАПН України, як власники важливих інформаційних ресурсів, лише частково стикаються з питаннями інформаційної безпеки і кіберінцидентів. Більшість інцидентів або не фіксуються системно, або недооцінюються через низьку обізнаність про реальні загрози. Недостатньо впроваджуються практики безпеки, такі як резервне копіювання чи організоване навчання персоналу, а рівень обізнаності працівників щодо політик кіберзахисту залишається критично низьким. Налагоджена комунікація щодо випадків кіберінцидентів фактично відсутня, що посилює ризики для збереження цінних наукових та освітніх інформаційних активів, особливо в умовах збройного конфлікту.

Рекомендації:

1. Терміново розробити та впровадити внутрішню політику інформаційної безпеки для всіх працівників наукових установ.

2. Організувати обов'язкове навчання з кібергігієни та цифрової грамотності, з урахуванням специфіки наукових та освітніх ресурсів.

3. Впровадити системну політику резервного копіювання критично важливих даних з регулярним аудитом її виконання.

4. Забезпечити відкриту внутрішню комунікацію про будь-які випадки кіберінцидентів, щоб підвищити рівень обізнаності та відповідальності в колективі.

5. Адаптувати інформаційну інфраструктуру до підвищених ризиків воєнного стану, зосередивши увагу на захисті та безперервності доступу до наукових і освітніх інформаційних ресурсів.

Список посилань

Міністерство освіти і науки України. (2023). *Інформаційно-аналітичні матеріали про можливості залучення наукових кадрів із статусом внутрішньо переміщених осіб до провадження наукової, науково-технічної та інноваційної діяльності.* https://mon.gov.ua/static-objects/mon/sites/1/nauka/2023/11/15/Inform-analit.mat.pro.mozhl.zaluch.nauk.kadriv.iz.statusom.VPO.15.11.2023.pdf

Національна академія педагогічних наук України. (n.d.). *Офіційний вебсайт*. https://naps.gov.ua

Kovalenko, V., & Lysenko, A. (2023). Cybersecurity challenges during the Russian invasion of Ukraine: Lessons for critical infrastructure. *Journal of Information Security Research*, *15*(2), 88–97.

Shevchenko, N., Melnyk, I., & Bondarenko, T. (2024). The role of cyber resilience in educational institutions during hybrid warfare in Ukraine. *International Journal of Cyber Warfare*, *(4)*, 103–119.

Datsiuk, O., & Voronova, L. (2025). Securing the digital future of Ukraine's education and science sector post-invasion. *Open Access Journal of Cyber Defense*, *3*(1), 14–26.

Shkuropadska, D., Tokar, V., Purdenko, O., Lotariev, A., & Savchuk, K. (2025). Digital resilience of the Bucharest Nine and Ukraine. *International Journal of Economics and Financial Issues*, *15*(1), 24–31. https://doi.org/10.32479/ijefi.17233

Shtantsel, S., Buryk, Z., Grytsyshen, D., Yevenok, O., & Sergiienko, L. (2025). Evaluating information security strategies in the public sector: Efficiency and cybersecurity risks. *Journal of Information Systems Engineering and Management*, *10*(2s). https://www.jisem-journal.com